The System Policies for the Recipient Update Service

By Marcelo Calbucci

Keywords: Recipient Policy, System Policy, Recipient Update Service, Mail Enable Recipient, Mailbox Enable User, Hidden DL Membership Policy, Non-Canonical Security Descriptor, msExchMailboxGuid, hideDLMembership, legacyExchangeDN

The Recipient Update Service has three System Policies that are installed by default when you install Exchange 2000. They are the “Mail Enable Recipient”, “Mailbox Enable User” and “Hidden DL Membership”. All of them have the same purpose of update a few attributes on each entry under certain circumstances.

The idea behind the System Policies is to let people to write their own tool to add and edit Users, Groups, Contacts, etc. To make the creation of these tools simpler, the Recipient Update Service takes part of the responsibility, filling gaps where a tool might have created, and on which case would cause other services to not work properly.

For a mail-enabled recipient, there is a minimum of attributes that is required to make all Exchange components to work properly. For instance, a mail-enabled entry (user, contact, group, public-folder, etc) need to have at least these attributes: mailNickname, legacyExchangeDN and displayName. Without the mailNickname an object is not considered a mail-enabled object. But once you have mailNickname you need also to have those other two attributes.

If the Recipient Update Service identifies that a new entry was added (or modified), and it does have the mailNickname to be considered mail-enabled, but it doesn’t have or legacyExchangeDN or displayName, it will try to stamp those attributes.

The displayName will be copied from the mailNickname as is, and the legacyExchangeDN will go thru an algorithm that identifies the Organization and Site for this entry, and create a value in the format

/o=MyCompany/ou=MySite/cn=Recipients/cn=MailNickname

For a Mailbox Enabled User, two things need to be present, one is the mailNickname, and the second is one out of three attributes: msExchHomeServerName, homeMDB or homeMTA. If any of those three attributes is present and the user has mailNickname, it is considered a Mailbox Enabled User.

On this case, we'll try to populate some attributes if not present, they are: msExchHomeServerName, homeMDB, homeMTA, legacyExchangeDN, displayName and msExchMailboxGuid.

If msExchHomeServerName is not present we'll create it based on the homeMDB or homeMTA, depending which one is present and on this order. If we fail to create this, we'll stop the process.

Once we have msExchHomeServerName we'll try to create the homeMDB and homeMTA if any of them are missing. On this case, if you have multiple MDBs or MTAs on your Server, it'll pick the first one that it finds doing a AD search, so it can be considered randomly.

To create the legacyExchangeDN and displayName we'll use the same steps that we used for "Mail Enable Recipient".

And finally, we might create an msExchMailboxGuid if not present, generating a random GUID.

For the "Hidden DL Membership" system policy, things are a little different because it is not only when you create a new entry (Group), but when you modify the status of the attribute "hideDLMembership".

If this attribute is set to TRUE, the Recipient Update Service will add a Non-Canonical part to the Security Descriptor, not letting people to see the "member" attribute for that entry. This will apply to any type of client searching the DS, thru MAPI or LDAP.

If the attribute is set to FALSE, it will remove the Non-Canonical Security Descriptor, exposing the "member" attribute again.